AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a pipeline microprocessor. In one embodiment, an apparatus is provided for accomplishing cryptographic operations. The apparatus includes a cryptographic instruction, CBC block pointer logic, ~~and execution~~execution logic, and a bit. The cryptographic instruction is received by a pipeline microprocessor as part of an application program executing on the pipeline microprocessor. The cryptographic instruction is prescribed according to the x86 instruction format and prescribes one of the cryptographic operations. The one of the cryptographic operations includes a plurality of CBC block cryptographic operations performed on a corresponding plurality of input text blocks. The CBC block pointer logic is operatively coupled to the cryptographic instruction. The CBC block pointer logic directs the computing device to update pointer registers and intermediate results for each of the plurality of CBC block cryptographic operations. The execution logic is operatively coupled to the CBC block pointer logic. The execution logic executes the one of the cryptographic operations. The bit is coupled to the execution logic, and is configured to indicate whether the one of the cryptographic operations has been interrupted by an interrupting event.

[0022] One aspect of the present invention contemplates a apparatus for performing cryptographic operations. The apparatus includes a cryptography unit disposed within a pipeline microprocessor, ~~and CBC block~~CBC block pointer logic, and a bit. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction within an application program that prescribes the one of the cryptographic operations. The cryptographic instruction is prescribed according to the x86 instruction format. The one of the cryptographic operations includes a plurality of

CBC block cryptographic operations performed on a corresponding plurality of input text blocks. The CBC block pointer logic is operatively coupled to the cryptography unit. The CBC block pointer logic directs the pipeline microprocessor to update pointer registers and intermediate results for each of the plurality of CBC block cryptographic operations. The bit is coupled to the cryptography unit, and is configured to indicate whether the one of the cryptographic operations has been interrupted by an interrupting event.

[0023] Another aspect of the present invention comprehends a method for performing cryptographic operations in a device. The method includes, via a cryptography unit within a pipeline microprocessor, executing one of the cryptographic operations responsive to receiving a cryptographic instruction, wherein the cryptographic instruction is prescribed according to the x86 instruction format, and wherein the cryptographic instruction prescribes the one of the cryptographic operations. The executing includes performing a plurality of CBC mode block operations on a corresponding plurality of input text blocks, and indicating whether the one of the cryptographic operations has been interrupted by an interrupting event. The method also includes writing a current input text block to an initialization vector location so that a following one of the plurality of CBC mode block operations on a following one of the plurality of input text blocks will employ the current input text block as an initialization vector equivalent.